Environmental Management Consolidated Business Center (EMCBC)

Subject: Policy on the Control of Unclassified Electronic Information

Policy Statement APPROVED: ***(Signature on File)***
EMCBC Director
ISSUED BY: OFFICE OF INFORMATION RESOURCES MANAGEMENT

1.0 POLICY**:** The purpose of this policy is to define the use and control of all Unclassified Electronic Information at the Environmental Management Consolidated Business Center and to define the reporting requirements for loss of control of Sensitive Unclassified Information.

2.0 APPLICABILITY**:** This policy is applicable to all electronic media managed by the EMCBC directly or by Service Level Agreement. This policy is not applicable to Classified Electronic Information.

3.0 REFERENCES**:**

3.1 Office of Management and Budget Memorandum, Protection of Sensitive Agency Information, dated June 23, 2006

3.2 DOE CIO Guidance CS-38A, Protection of Sensitive Unclassified Information, Including personally identifiable Information, November 2006

4.0 DEFINITIONS**:**

4.1 IRM – EMCBC office of Information Resource Management.

4.2 Electronic Information – Any information stored or transported on electronic media such as hard-drives, flash drives, CDs, DVDs, etc.

4.3 Sensitive Unclassified Information (SUI) – Unclassified information requiring protection mandated by policy or laws, such as Official Use Only (OUO), Export Control Information (ECI), Unclassified Controlled Nuclear Information (UCNI), Naval Nuclear Power Information (NNPI), Personally Identifiable Information (PII), and other information specifically designated as requiring SUI protection such as information identified under Cooperative Research and Development Agreements (CRADA).

4.4 System Owner: The lead IRM individual that has overall implementation responsibility for any given Application, System or Accreditation Boundary. Usually this is the Assistant Director for Information Resource Management.

4.5 Content Owner: The Assistant Director responsible for the content within the given application or system.

4.6 Content Manager: Individual assigned by the Content Owner to manage the development of applications and to ensure data integrity.

5.0 GENERAL INFORMATION**:**

5.1 Policy**:** All forms of electronic data will be reviewed for sensitivity and applicable controls will be applied. Applicable controls come from references (a) and (b), and this policy. It is the policy of the EMCBC that all electronic information is controlled as required. Excessive controls are cumbersome and unduly impact business operations and are to be avoided. Where data types are mixed, the most stringent control shall apply.

5.2 Data Sensitivity and Controls**:** Data within the EMCBC is classified by type according to the sensitivity of the data.

- Type I Data – The data in this category requires the most stringent control and is made up of the most sensitive data. All Sensitive Unclassified Information (SUI) falls into this category and the controls identified in reference (b) apply to all Type I data. Other data may be designated as Type I by the Content Owner if necessary to meet a particular need. These controls mandate:
    - All SUI shall be stored on network peripherals. SUI shall not be stored on Desktops.
    - All data storage on laptops, USB drive, CDs, and DVDs shall be encrypted
    - All SUI stored on any mobile devices including portable hard drives shall be encrypted.
    - SUI is encrypted before transfer over open connections. EMCBC uses Entrust for this purpose.
    - Data access within the accreditation boundary is controlled through network authentication.
    - Remote access to EMCBC file storage and applications containing SUI shall utilize two factor authentication and conform with the time-out requirements of reference (b).
- Personally Identifiable Information (PII) is a special form of Type I data and requires additional controls over and above those already stated.
    - PII is not permitted to be stored on Desktop computers, laptops, USB drives, DVDs, CDs or any other forms of portable media. In unusual circumstances PII may be stored on portable media with the written

authorization of the Director, EMCBC. Such authorizations will expire after 90. At such time the media will need to be returned to IRM for disposition or renewal of the authorization is required. Personnel authorized to transport such data will be required to receive additional training to ensure a full understanding of the ramifications of transporting PII.

- Annual Cyber Security Awareness training, required for all users, will describe PII in detail to provide a clear understanding to all users on the special restrictions and rigorous reporting requirements for PII.

- Type II Data – Information in this category is designated by the Content Manager or Content Owner. The data is usually made up of sensitive business information that if compromised could lead to an unfair competitive advantage, divulge sensitive legal position, or expose other confidential information. The Content Owner is responsible for the designation of all Type II data. The following controls apply:

  - Data access within the accreditation boundary is controlled through network authentication.

  - All data stored on laptops shall be encrypted.

  - USB Flash Drives and other portable media shall be protected by encryption.

  - Remote access to EMCBC file storage and applications containing Type II data shall utilize two factor authentications and conform to the time-out requirements of reference (b).

- Type III Data – Information in this category is designated by the Content Manager or Content Owner. The goal of this is to protect data integrity, and add level of confidentiality, or screen information from the general public. Certain types of Business Sensitive Data may fall into this category. The following controls apply:

  - Data access within the accreditation boundary is controlled through network authentication.

  - USB Flash Drives and other portable media shall be protected by password protecting the file.

  - Remote access shall require authentication by username and password.

- Type IV Data – information that is or can be made available to the general public without restriction. Data integrity to ensure accurate communications is the goal of this information control. The following controls apply:

- Data access within the accreditation boundary is controlled through network authentication.

- Data posted to websites is controlled by the Content Owner or Content Manager.

- Data integrity for web servers and other public facing information systems is maintained by the security controls imposed by the System Owner as part of the Accreditation Boundary.

5.3 Reporting of Data Security Issues**:** All users responsible for the control or transportation of Type I and Type II Data shall immediately report any loss or potential compromise of the data to the Assistant Director for Information Resource Management. This reporting shall be done within 30 minutes of any possible loss or breach of Type I Data. All response to loss of data control will be handled by Information Resource Management in accordance with Incident Response procedures.

5.4 Training**:** All users handling Type I and Type II Data shall receive specific training in the use of encryption and data protections systems. All laptop users will receive training on use of laptop locking and encryption devices and systems. General User training will address the controls for Type III and Type IV Data.

Summary Chart on Controls for Electronic Information

Type	Definition	Control
I-PII	Data defined as PII by regulation or requirement	Data is only stored on network storage devices. Access is controlled by network credentials. Special authorization required for transportation on mobile devices. Users receive special training to ensure protection of this data.
I	Data that has been specifically defined as needing encryption by requirement such as Sensitive Unclassified Information	Data is stored or transported encrypted as required and, requires two factor authentication for remote access. Users receive special training to ensure protection of this data.
II	Business Sensitive Data – data that has a direct bearing on business decisions that if compromised could result in an unfair advantage to parties conducting business or in legal action with the department. Type II data is designated by the Content Owner	Data access is controlled through the network and requires two factor-authentications for remote access. Data is protected by encryption in transport.
III	Information about Business Sensitive Data that requires protection to ensure data integrity, and a level of confidentiality, or data needs to be screened from the general public. Type III data is designated by the Content Owner	Data access is controlled through the network, requires username and password for remote access. Files transported on removable media should be protected by password.
IV	Public data that may be released at anytime. Web site data makes up the bulk of this data.	Data access is controlled through the network. Data is posted to the web as directed by the Content Manager. Precautions are taken to ensure data integrity.

EMCBC RECORD OF REVISION

DOCUMENT - **Policy on the Control of Unclassified Electronic Information**

If there are changes to the controlled document, the revision number increases by one. Indicate changes by one of the following:

- Placing a vertical black line in the margin adjacent to sentence or paragraph that was revised.
- Placing the words GENERAL REVISION at the beginning of the text.

Rev. No.	Description of Changes	Revision on Pages	Date
1	Original Procedure	Entire Document	1/18/07
2	Clarify that all SUI on any mobile devices must be encrypted	Page 2	6/16/08
2	Separate PII is a special form of Type I with additional controls	Page 2, 3, 5	6/16/08
Periodic Rev.	Completed periodic review with no changes.	No changes	6/10/10